Pages 1 - 72

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

Before The Honorable Richard Seeborg

ANIBAL RODRIGUEZ, et al.,	)	
	)	
Plaintiffs,	)	
	)	
VS.	)	**NO. 3:20-cv-04688 RS**
	)	
GOOGLE, LLC,	)	
	)	
Defendant.	)	
	)	

San Francisco, California
Thursday, July 25, 2024

TRANSCRIPT OF PROCEEDINGS

APPEARANCES:

For Plaintiffs:

BOIES, SCHILLER & FLEXNER, LLP
333 Main Sreet
Armonk, NY 10504
BY: DAVID BOIES
ALEX BOIES
ATTORNEYS AT LAW

BOIES, SCHILLER, FLEXNER, LLP
44 Montgomery Street, 41st Floor
San Francisco, CA 94104
BY: BEKO OSIRIS REBLITZ-RICHARDSON
MARK C. MAO
ATTORNEYS AT LAW

(Appearances continued on next page)

REPORTED BY: Rhonda L. Aquilina, RMR, CRR, CRC
CSR No. 9956, Official United States Reporter

APPEARANCES cont'd.

For Plaintiffs:

BOIES, SCHILLER, FLEXNER
100 SE 2nd Street, Ste. 2800
Miami, FL 33131
BY: JAMES W. LEE
ATTORNEY AT LAW

BOIES, SCHILLER, FLEXNER, LLP
2029 Century Park East, Ste. 1520
Los Angeles, CA 90067
BY: M. LOGAN WRIGHT
ATTORNEY AT LAW

SUSMAN, GODFREY, LLP
One Manhatan West
395 9th Avenue, Ste. 50th Floor
New York, NY 10001
BY: ALEXANDER PATRICK FRAWLEY
RYAN SILA
ATTORNEYS AT LAW

MORGAN AND MORGAN, P.A.
201 N. Franklin Street, 7th Floor
Tampa, FL 33602
BY: JOHN A. YANCHUNIS
RYAN MCGEE
ATTORNEYS AT LAW

For Defendant:

WILLKIE, FARR & GALLAGHER, LLP
333 Bush Street
San Francisco, CA 94104
BY: EDUARDO E. SANTACANA
BENEDICT Y. HUR
ARGEMIRA FLOREZ
SIMONA A. AGNOLUCCI
ATTORNEYS AT LAW

Thursday - July 25, 2024 **1:28 p.m.**

P R O C E E D I N G S

---o0o---

THE CLERK: Calling case 20-CV-4688, Rodriguez versus Google.

Counsel, please state your appearances.

MR. BOIES: Good afternoon, Your Honor. David Boies from Boies, Schiller & Flexner on behalf of plaintiffs.

THE COURT: Good afternoon.

Go ahead.

MR. MAO: Good afternoon. Mark Mao, Boies, Schiller.

MR. LEE: Good afternoon. James Lee, Boies, Schiller.

MR. YANCHUNIS: Good afternoon, Your Honor. John Yanchunis with Morgan and Morgan.

MR. SILA: Good afternoon, Your Honor. Ryan Sila from Susman, Godfrey.

MR. McGEE: Good afternoon, Your Honor. Ryan McGee from Morgan and Morgan.

THE COURT: Good afternoon.

MS. SANTACANA: Good afternoon, Your Honor. Eduardo Santacana of Willkie, Farr & Gallagher for Google. And I have counsel here who can introduce themselves. We also have in-house counsel from Google.

MR. HUR: Good afternoon. Ben Hur also from Willkie, Farr.

MS. AGNOLUCCI: Good afternoon. Simona Agnolucci also from Willkie, Farr.

MS. FLOREZ: Good afternoon. Argemira Florez, also from Willkie, Farr.

THE COURT: Good afternoon. So we are here on Defendant's Motion for Summary Judgment.

I will look to the moving party to start the discussion. I don't -- I think you may have provided or some indication you've provided some additional material in the form of demonstrative, I guess we can call it, items. Generally I don't like those for motion arguments. It's not that parties intend this, but it is a bit of an end run around our page limits. In patent cases I've given up because they use it in every single one, Power Points and other things.

I won't preclude you from using it, and you can make reference to it, but certainly for consideration of the motion I'm not going to be relying on any of the materials that you use in that fashion, because at best they are demonstrative materials.

Okay. So if the moving party wants to begin.

MS. SANTACANA: Thank you, Your Honor.

I'm actually not aware of any demonstratives on either side in this matter.

THE COURT: Oh, good.

MS. SANTACANA: I don't know if the plaintiffs have

any, but we do not.

THE COURT: I thought I was told that somebody had submitted some materials, but maybe I'm mistaken.

Okay. Go ahead. So you're not patent lawyers, so that's great.

(Laughter)

MS. SANTACANA: Not today.

Your Honor, there are three central reasons why this case should be dismissed. First, Google said what it meant and it did what it said. Second, to the extent Google didn't get the language exactly right, what it did do with the data in question was harmless and not highly offensive. Third, Google's intent, backed up by major investments and safeguarding pseudonymized user data, cannot give rise to liability under the two remaining claims in the case.

I'll turn first to consent.

Google's internal view of the WAA button was exactly what it told users it was, that the button should control whether app activity data is saved to a user's Google account or instead treated as non-personal information.

THE COURT: Let me just stop you on this. What constitutes personal information and what would a user understand that characterization to be?

You take the position that it's just crystal clear that if you read through your privacy policy any user is going to

understand the distinctions that you're drawing. But on what do you base that?

I mean, this label "personal information" and that being what, you think the user understands is the only thing that's not being shared; is that really reflected in your privacy policy materials?

MS. SANTACANA: It is, Your Honor. And I want to make one preliminary point before answering your question, which is that to the extent a user is unclear about what personal information is and is not, it's not clear to me that that should inure to Google's detriment here, and the reason for that is because Google secured an underlying express consent for the data collection in question, which is basic ad recordkeeping collection and analytics customer servicing.

The question here is whether the plaintiffs clearly withdrew their consent after giving it to Google by turning WAA off.

THE COURT: I mean, they made their -- the users, who are the class members here, made it known in no uncertain terms that they didn't want some of their information shared. Now, whether or not, as you say, they should have been clear on what's being saved and not, we can all agree that --

MS. SANTACANA: Yes.

THE COURT: -- these class members took the affirmative step of switching off the --

MS. SANTACANA: Yes.

THE COURT: -- the two switches, if you will.

MS. SANTACANA: Yes. And if you look at their briefing, every single time they talk about scope of consent, they say that the legal standard is consent is not an all-or-nothing proposition, you have to look at the context, it might be yes for this and no for that. And so the same applies when we're talking about withdrawal of consent. They asked to withdraw consent for something. The question is how broad is that scope.

So your specific question was, what is the definition of "personal information?" How do they know the difference between personal and non-personal information? It's actually right in the privacy policy. The first paragraph in the privacy policy says if there's anything in here you don't understand, click here, read the key terms definitions.

There's three key terms that are relevant to this motion. the first is "Google Account," the second is "non-personally identifiable information," and the third is "personal information," which is where I'm going to start.

So, the WAA button says it controls what is, quote, saved to your Google account. The definition of personal information says this is information which you provide to us which personally identifies you, such as your name, email address, your billing information or other data which can be reasonably

linked to such information by Google, such as information we associate with your Google account. Associate with your Google account.

So here, again, Google is mirroring the language in the WAA control, and it does it all throughout the privacy policy, right? In the main body of the privacy policy, what Google says is this is what a cookie is, this is what similar technologies to cookies are. And we say information we collect when you're signed in, in addition to information we obtain from partners, quote, may be associated with your Google account. When information is associated with your Google account, we treat it as personal information.

This is unlike page 4 of the privacy policy.

THE COURT: What does "associated with your Google account" mean? I mean, I may have this wrong, and plaintiffs can correct me, but I thought the plaintiffs were suggesting that some of the information at issue here does link up with certain devices. I know you say it's all anonymized and nobody can figure out exactly who is involved here, but it does link up to -- there's some information that links up to particular devices, doesn't it? And those devices are then connected to people, right?

So why is it that it -- you say it can't, as a matter of law, because we're in summary judgment, and you're saying there's just no dispute about it, that there is no way that the

information that's at issue here can be in any way associated, and that was the word you just used, with individuals.

MS. SANTACANA: Well, again, the question is not could it be associated with your personal information or could it be associated with your Google account. This is not a case about the theoretical conduct Google could have engaged in.

THE COURT: Why not? I mean, if you are collecting information that could be used for that, why wouldn't that be relevant in this case? You're saying it has to have been used in that fashion to link back up to individuals?

MS. SANTACANA: Of course, Your Honor, because otherwise it's a theoretical concern. So Google --

THE COURT: There may be value -- plaintiffs may view that they have, class members, that there's value in that information because it could be used in that fashion.

MS. SANTACANA: That may be the case, but that doesn't mean that Google has engaged in an intentional invasion of privacy or a violation of the CDAFA.

So if we're looking at the legal claims in question, Google actually has to engage in invasive conduct. The fact that it could happen one day if a bad actor circumvented Google's protections --

THE COURT: But I think you're looking at it from the wrong perspective. It's not what theoretically could happen or not. It's what information is being -- is being accessed.

You're saying you are telling the user nothing that can be associated with you is being collected, and now you're sort of saying, well, theoretically, if it is used in a particular way it could connect up to an individual user.

MS. SANTACANA: No, Your Honor. I'm actually -- I'm not saying either of those things.

THE COURT: Okay.

MS. SANTACANA: So Google's WAA control doesn't say what -- the way you just phrased it. What it says is give us permission to save data in your Google account. The question is did Google save it in your Google account or not.

Now, what Google -- and I think it's undisputed that Google isn't saving it in your Google account. That's why five times in their brief they put an ellipsis in that phrase rather than actually use it, because they don't want to focus the case on that.

It is undisputed that Google doesn't save it in your Google account and doesn't associate it with any reasonable definition of personal information. In fact, the California legislature has in the CCPA already embodied this idea that you can de-identify and pseudonymize data by attaching it to an identifier that is randomly associated and that is not connected to a person's identity. That's the representation that Google made. That's the only representation that Google should be responsible for here today, because that's the basis

of the case.

I think to some extent what Your Honor is asking is more of a policy question. But the specific disclosure in the button says "saved data in your Google account."

Now, the second part of your question was, you were saying our argument is, well, it could be, but it hasn't been. That's not our argument. Our argument is that it cannot reasonably be linked. Why? Because Google -- first of all, Google created the system that exists, right? This system is there because Google created it. It has a privacy policy that discloses that it will collect certain information, and it has this button that says what it will and won't do with that information, right? In this case app activity data.

That same system prohibits the connection from one to the other. And there's no allegation in the case that there's a data breach or that Google sold it to a third party. None of that is in this case. There's no evidence of that.

So what we're talking about is Google creates two buckets, and it successfully kept the buckets apart. In the words of their expert, Google has attempted, with the best of intentions, but who knows maybe one day they turn evil. That's what he says in his deposition: "Maybe one day they turn evil."

But right now, looking back for past damages, the two buckets have remained separate. The system worked.

And I want to be very clear about this. If the plaintiffs had identified any example of Google failing at keeping those buckets apart, of Google connecting this data, quote, associating it with personal information under any reasonable definition, they would be jumping up and down screaming about it in their brief; they would be jumping up and down screaming -- I don't know if Mr. Boies jumps up and down and screams, but somebody would be doing that. I don't think there's any evidence of that. There's -- it's not in their brief. They never found any instance of that ever happening.

Instead, what they did was they theorized that there are concerns within Google or within their expert's opinions that it could be done by a bad actor, one day, if Google's systems were to change.

This is a case about Google's class-wide conduct. It is a case about past damages, and so in the past Google didn't do that.

THE COURT: Okay.

MS. SANTACANA: The other point I want to make about consent, Your Honor, before I turn to harm, is that when we're talking about the description of WAA, at the motion to dismiss stage Your Honor held that the definition of Google account was nebulous at best.

I want to be -- I want to read to you what Your Honor was evaluating at the time, because I think it is lost in the

briefing. The opposition to the motion to dismiss the first amended complaint, parroting the allegations of the first amended complaint, was arguing that Google was associating, quote, that data with Google's preexisting profiles thereby enriching those profiles with data Google was not supposed to have, and that Google services target users based on this data.

Now, it was in that context -- and there's more in the brief, but it was in that context, this idea of a shadow, quote, not your Google account, that Your Honor said, well, "save to your Google account" is nebulous if what you're saying is there's some shadow account that you're keeping that just doesn't have your name on it. That's not the case anymore. They were unable to find any evidence that Google ever personalized advertising or built marketing profiles using this data.

What they found, which we told them from the beginning in an interrogatory response four years ago, was we do keep records that we serve ads. That's it. We have a randomly assigned string of characters. It is not connectable to a person's identity, and it indicates that that device, that string of characters was served and added a particular time so that we can charge advertisers for it.

And they come and they say, well, the fact that you're keeping the receipt means that you're using the WAA-off data. And since you're using the WAA-off data, if I were to disable

you from keeping the receipt, you couldn't charge, and so every single penny of what you've charged needs to be disgorged. That's where we are now.

And so when we're talking about the scope of withdrawn consent, the question has to be could a reasonable user believe that when they turn WAA off, they not only disabled Google from saving personal information, but they disabled Google from saving a non-personal list of service of ads that is basically just a ledger of receipts.

And our argument is there's no reasonable user who could -- there's no reasonable reading of the language to support that. There's no phrase in the privacy policy or in the description of WAA to support that view. And without a textual hook, I think on the language by itself Your Honor can grant summary judgment.

Turning to harm, Your Honor, these two claims require --

THE COURT: Going back for a second to consent.

MS. SANTACANA: Sure.

THE COURT: And this is maybe just a variant on my first question, but effectively what I understand the plaintiffs to say is that the -- a reasonable consumer is left with the notion that nothing associated with me -- if they exercise the affirmative decision with respect to the buttons and say I want out of this -- that nothing associated with me, anonymized or otherwise, anything that you have retrieved about

me is not going to be shared, that that is their reasonable understanding.

And you've gone through -- and I understand it -- a fairly sophisticated analysis of what, you know, the material that ultimately may flow to the advertisers or whatever really is so generalized as to be almost not, in a sense, associated with the individual. But from the individual's perspective don't you think that at least it is fair that the user thinks nothing associated with me, be it anonymous or otherwise, is going to be shared? Isn't that a fair understanding of what you think the reasonable consumer thinks when they are electing those buttons?

Now, you could say yes to that and say we still win. But isn't that fair?

MS. SANTACANA: No, Your Honor, it's not fair.

THE COURT: Okay. And you really then think that they -- that the minutiae of your privacy policy is what the reasonable consumer should understand all of the -- and if they have a question, they can go ask and this, that, and the other thing -- that's really your position then, that the idea that a consumer walks away with the notion that they're just telling you don't, don't share anything at all about me, that that is just -- they're wrong, they, you know, it's on them to understand it more. I mean, what is it?

MS. SANTACANA: So I have several responses, if I may,

Your Honor.

THE COURT: Okay. It was a rambling question, so that's fair.

MS. SANTACANA: So first I want to make sure that we are taking the appropriate 30,000-foot view on this question, okay?

Google is a big company. It has lots of privacy buttons, about 13 of them, I think. Data comes in from various sources just like the WAA button says, as well as some other buttons that control other sources of data. It has a billion users worldwide, and it speaks to those users, or some subset of them, effectively every day through a variety of products - all of which are free and are self-serve, so anybody can come, agree to the thing, and start using it.

So Google has to find a way to explain technology, which we can all agree is sometimes not that easy to explain to a reasonable user as best as it can. And I don't think that a half billion-dollar jury trial is called for every time Google fails to use the perfect words to describe itself.

So when you're talking about the user who thinks "I told you nothing associated with me, whether personal or anonymized should be saved," my question is based on what? Which language are you relying on, Reasonable User, to believe this?

Because when I look at the language, that is not what it says. And it's not that it's not what it says in some

legalese --

THE COURT: Let me stop you there. That's where -- and I understand you -- I know what your answer was going to be. But we are at summary judgment, so what you think is a reasonable interpretation is a perfectly legitimate analysis on your part.

But what you really have to convince me of is that no reasonable person could have a contrary view, because unless and until you do that -- and I understand you say, well, the specter of every time -- I forget your language -- every time we're at a point that we've reached here, that the alternative for Google is a bazillion-dollar trial -- well, I'm not sure I entirely buy that. There are places along the path that they -- it doesn't automatically mean you go from point A to a bazillion-dollar judgment.

But going back to what I'm saying, you know, am I right that I have to effectively say your view is not only reasonable, but it is the only reasonable view?

MS. SANTACANA: No, I don't think you have to say that.

THE COURT: Okay. Why not, on summary judgment?

MS. SANTACANA: Because the standard on -- what we're talking about is the written word. And so generally in this area of the law, although a recent Ninth Circuit panel noted repeatedly that actually it's very unclear what the standard is

in California on privacy consent. But mostly we look at contract principles to understand what the written language is supposed to mean.

Here, I'm looking at the language -- and Your Honor has done this at summary judgment before -- you know, *Pacific Drayage*, California contract law. It's black letter law. We're going to start with the plain language. Does the plain language support reasonable -- is it reasonably susceptible to the plaintiff's view of it? That's the question. It's not that I have the only reasonable view of it. I might be able to give you 15 reasonable views of the language, but if none of them is reasonably susceptible to the plaintiff's view, then the plaintiff's lose. That's the standard.

THE COURT: Okay.

MS. SANTACANA: And so when I look at this language -- it's the paragraph at the top of the WAA button that they have in their complaint -- this is what it says, and I'm just going to read it because I'm going to make sure that we're focused on the plain language: "The data saved in your account helps give you more personalized experiences across all Google services. Choose which settings will save data in your Google account" and then it says Web and App Activity, and then there's some more words about all of the different types.

The user that you're positing who says, well, I thought that button means nothing, it's as though all Internet

connection between my -- google android device, by the way, this is an android device -- my Google android device and Google is severed completely, is not realistic or reasonable. No -- it's just not reasonably susceptible to app use.

So now we're at, okay, fine, so we agree with that. Obviously, the android device has to communicate with Google somehow about some thing. Google is going to save some of that. And the question is fine then what's the scope? Now we're talking about scope. And does it include marketing profiles? Yeah, maybe. I don't think we would get summary judgment on that. But there are no marketing profiles that Google is saving when WAA is off.

Does it include an anonymized list of which ads were served which Google uses solely for the purpose of charging advertisers? I don't think a reasonable user -- I don't think there is a reasonable reading of this language that would say that. But if there were, at a minimum we would need to click on the "learn more" button and look at the privacy policy.

And the privacy -- you said minutia, I really -- I don't agree with that. The privacy policy over and over and over again draws a conceptual distinction, as best as Google can with a billion users talking to them every day, constantly changing privacy policy, but over and over they're saying there's such a thing as personal information, and there's such a thing as non-personal information, and they do their best to

say personal information, non-personal information are different. You can control this one, you can't control that one.

So the necessary implication is there's something I can't control, and does ads recordkeeping fall under this one or that one, is the question. Is it reasonably susceptible to the view that it's the same as a marketing profile? No. I really -- it doesn't fit. But if Your Honor doesn't agree with that, then we have to look at harm.

And on the question of harm, as I said, there isn't a single piece of evidence in the case that Google ever associated this ledger of ad receipts, or for that matter the analytics data that's in this virtual safe deposit box for analytics customers with a person's identity, when WAA was off.

And because there's no evidence of that, even if we assume that the expectation of privacy that is given rise to by the WAA button includes anonymized data, the question is, well, is it highly offensive to keep a receipt for the ads you serve and only use it for that? Is it highly offensive or does it cause actual damage or loss, which is an even higher bar in CDAFA. It has to be actual damage loss. Does it cause actual damage or loss for Google to keep a record of what it does when it services an advertising account?

Under both of the remaining claims in the case, there's no CIPA claim, there's no UCL claim, these are --

THE COURT: Yep.

MS. SANTACANA: -- these claims require a showing of real harm.

Where the plaintiffs have landed in their opposition brief is to rely on things like battery depletion and emotional distress. They say the harm from the invasion of privacy itself satisfies the harm requirement of invasion of privacy. That's not true. It's not true.

Now, the reason this doesn't come up in an invasion of privacy tort case very often is because an individual plaintiff can say you hurt my privacy and it caused emotional distress. At class cert. they disclaimed any reliance on that.

So then they say in the opposition brief: Well, what about batteries? My battery is being depleted. Under *Comcast versus Behrend*, the Supreme Court case on class action damages, the damages model they present at class cert. has to be tied directly to the way in which they say the conduct gives rise to liability. The liability theory must match the damages model. There's no damages model on battery depletion, so they can't proceed on that. We' have to redo class cert., and honestly I think they're precluded at this point. It's been four and a half years.

So then we have to talk about the damages models that they do have and this question of disgorgement.

So, again, the theory of the case on disgorgement is if

the restaurant serves you pancakes and you pay for the pancakes, and it keeps a receipt and I told them no, you can't keep receipts, then the entirety of what's paid for the pancake must be disgorged, because you couldn't possibly charge for the food if you didn't have the ability to keep the receipt. That's the argument. The receipt is the WAA-off data.

Under *TransUnion*, which postdates the *Facebook Internet Tracking* case, that is not sufficient to satisfy the statutory standing requirement under a statute like CDAFA, and it's not sufficient to the actual harm. The fact that the receipt may have business value to Google does not amount to a harm to the user.

And what's interesting is there's no actual testimony in the case from a user, like a plaintiff or one of the five who withdrew, that says I'm hurt by the fact that you kept a receipt for advertising. Each plaintiff, what they testified to, was: I am hurt by the fact that you targeted advertising to me. Because they were under the false pretense that that was actually happening.

So the first person to ever identify the ad recordkeeping activity as a problem was a lawyer on the plaintiff's side. No employee of Google ever brought it up, no plaintiff ever brought it up, nobody has ever brought it up, because it would never occur to anybody that that could cause harm to a person or be highly offensive or breach social norms.

The cases on offensiveness and harm, including Your Honor's own cases, were evaluating, the ones we cite in the papers, were evaluating data collection that was far more detailed than this. Your Honor decided the *Williams* case in 2018 and the *Katz-Lacabe* case last year; there's also the *Williams versus DDR Media* case by Judge Illston, the *Low versus LinkedIn* case by Judge Koh, the *Hammerling* case, which was affirmed by a panel of the Ninth Circuit on March 5th, and the *McCoy* case, which is related to the *Hammerling* case, which was decided in 2021 by Judge van Keulen. All of those cases evaluated data collection that included information, just to use *DDR Media* as an example, information like every keystroke entered on a web site associated with an identifier that was de-identified.

And even there each one of those judges, including Your Honor, said this isn't highly offensive; this is routine, commercial behavior or not even, because it's de-identified.

The California legislature has passed a law now, since this case was filed, the amendment to the law that says de-identifying is a legitimate way to protect data. Pseudonymization is a legitimate way to safeguard user data, which is what Google is doing. So if we're looking for clues as to what is or is not highly offensive, that's another one.

What is not in the papers is any case that comes anywhere close to the facts of this one where it is found to be highly

offensive. And there's two cases in our reply brief I want to call your attention to if you're looking for binding authority. *Eichenberger versus ESPN* is a Ninth Circuit case from 2017. That case is actually a lot like this one. In that case what was alleged was that a Roku, which is a smart TV appliance for televisions, a Roku was recording the serial number of the device and the names of the videos that the user was watching.

Here, we're not even doing that. We're recording the serial number, the device, and the randomly served ad, which the user has no real private expectation in any way. I mean, even if we were to proclaim from the rooftops that a particular person was served a particular ad, it's not clear to me that there's anything private about that.

But in any case, Roku is the device, serial number, and the names of the videos the user watched. And the Ninth Circuit said that's not highly offensive. That's routine, commercial behavior.

The second one is the *Zynga* case in 2014, which on these facts is much more like this case than the *Facebook Internet Tracking* case from 2020, which is the one Your Honor was following at the motion to dismiss stage when the allegation was that we were keeping browsing histories to personalized advertising.

The last thing I'll say, Your Honor, is about intent. And this one is I think near and dear to my heart as somebody who

has worked on this case for so long.

Google -- the evidence in this record is that Google had an internal understanding of what the button was supposed to do and it followed it. It set up all these systems to make it happen. We had 14 people from Google, former and current employees testify, all said the same thing.

These systems were put in place to safeguard user data and user privacy. That was Google's subjective understanding of what it was attempting to do. The two claims that remain here are not strict liability claims. They require intent. They require the intent that is missing when you take into account just two facts.

Google summarized its own understanding pretty well about what it was trying to do. It may not be perfect. It may not be enough for Your Honor to grant summary judgment on consent. But they did summarize it in a way that is perfectly consistent with what they were trying to do, and they did it at a massive cost, leaving much money on the table that could have been used, that could have been made if they had personalized advertising with this data, which is precisely what the plaintiffs alleged we were doing, falsely.

So if Your Honor is to say that a reasonable juror could find intent, my question to the plaintiffs would be based on which fact?

And for them, what they say is, well, there's employees

who understood that WAA was confusing in one way or another way. What I want to be really clear about, Your Honor, is not one of them, not one of them ever thought about this. They weren't thinking about Google keeping a record of which ads it serves or which conversions are made. When they said that it was confusing, one of them said it was confusing because it was -- the dutch translation wasn't very good. Another one said it was confusing because it wasn't clear what it means when the WAA button is on.

The fact that it is sometimes confusing to some people about something else does not manifest intent on the part of the company, which has spent millions to do exactly what it thought it had said it was going to do. It doesn't manifest corporate intent that there is this other set of people, individuals who are a little unclear about other aspects of the button.

So with that, Your Honor, I'll yield.

THE COURT: Well, just while you're on intent, and, again -- well, this doesn't really call into question what you've just said, but as a general matter I think you would agree granting summary judgment on intent is disfavored, if you will.

MS. SANTACANA: Agreed. Completely.

THE COURT: You think this case on the intent issue is so strong on your side that it's subject to summary judgment.

MS. SANTACANA: I -- I don't -- it's incredibly strong because, as I said, the company put its weight behind its subjective intent, and its subjective intent is consistent with the language on the button and in the privacy policy. So there isn't really a hook to say, oh, the company is trying to --

Like, for example, if the plaintiffs had demonstrated that the company was secretly profiting off this data by using it to target advertising, that would be a very different case. That's more like the case Your Honor let through at the Rule 12 stage.

Google isn't doing anything with the WAA-off data. It is using it to keep a record of the ads that it served. It's servicing analytics customers' accounts for free. It is not using the data to enrich itself or understand better its own users.

So where is the fact that's giving rise to even the plausible thought that there is intent. It is disfavored.

Last week, Your Honor, Judge Chhabria held at the motion to dismiss stage that the plaintiffs had failed to allege, in an analytics case, had failed to allege enough facts to meet the intent standard, because Google publicly says we are not going to use data for health-related advertising. This is in the *Doe versus Google* case, which we can submit to Your Honor if you're interested. And the plaintiffs had no basis to argue that that was a lie.

Here, it's the same thing. Where is the basis to say Google had secretly had a different intent that was sufficient to give rise to an intentional tort for invasion of privacy, which is typically reserved for some pretty serious conduct, or a violation of a state anti-hacking statute.

I agree with the plaintiffs that the intent to do what you set out to do can sometimes be enough. But when -- but here, the intent has to be read in the context of the disclosures that Google made. So Google says I'm going to do this, and it does that. And the plaintiffs say, well, I didn't totally understand what you meant. Nobody else has ever taken the same interpretation as the plaintiffs. Does that really give rise to liability?

THE COURT: Okay. I'll give you an opportunity to respond, because you're the moving party, but I'll look to the plaintiff, Mr. Boies.

MS. SANTACANA: Thank you, Your Honor.

MR. BOIES: Thank you, Your Honor. And may it please the court, my name is David Boies.

Let me begin with the issue of intent, Your Honor, because --

THE COURT: Aha! Some materials.

MR. BOIES: These are things I'm going to be referring to, but they're, for the most part at least, not demonstrative, so they're the actual evidence. For example --

THE COURT: Okay. All right.

MR. BOIES: -- I'm going to point you to the beginning.

If we could go to chart number 2, because I want --

THE COURT: Well, I won't quibble with you, but it -- we have things like statements that look like Power Points and things.

MR. BOIES: There are some Power Points.

THE COURT: It's fine. I gave my spiel. You know my general view of this for motion argument, but I'm not precluding you from using it. So go ahead.

MR. BOIES: Thank you, Your Honor. And I'm not relying -- I'm not offering anything here except the actual evidence.

THE COURT: Okay.

MR. BOIES: But the actual evidence is really critical here, because you've heard a lot about what they think their evidence is going to show. But, respectfully, since this is a summary judgment motion and they're the moving party, what's really relevant is the evidence we're relying on.

The question is not whether they have evidence from which they can make arguments. The question is whether we have evidence that creates a triable issue of fact. And so you've got to look at what the actual words are, because we don't think the actual words are what they were saying the words are.

I mean, for example, they said: All we ever promised to do is not save personal information. That's not what their documents say, and I'm going to take you through it.

THE COURT: Well, I assume your position is even if that was --

MR. BOIES: Even if that was the case, we think they save personal information because, as they have said themselves, if it can be reasonably -- could be, could be, not it were, but could be reasonably linked, that's personal information. That's what the California statute says. That's what their definition says. And there's no doubt here that they can do it. Their expert admits it. Our expert says so, and their internal documents say that they do it.

So they may say that they have these safeguards to prevent people from -- bad actors from doing it. But there's no dispute in the record -- there's certainly far more than necessary to create a triable issue of fact -- that they could reasonably link this --

THE COURT: So what do you say to Mr. Salcedo's (sic) point that until they do it, no harm, no foul?

MR. BOIES: Because, Your Honor, what they've done is they've collected this very personalized information. And if you look at our expert report, Mr. Schneier, paragraph, I think it's 89 --

Let me see number 73, because I think I've got it. I

think I quoted it. It's page 73 of what I've given you, I think.

Can we put that up? No? Maybe. Can we put up number 73?

THE COURT: Well, I'm on your -- the Schneier report, 73.

MR. BOIES: Yes.

THE COURT: It's paragraph 89.

MR. BOIES: Exactly.

THE COURT: Okay.

MR. BOIES: And if you look at that, you see the kind of information that is being collected. Now, they may say they don't use that information. They may say -- although I think the evidence is that they use at least some of that information. But this is the kind of information that is being collected, and that is exactly the kind of information that we think is highly offensive to people, particularly when they're told that information is not going to be collected.

Now, in addition, unlike the cases that they cite --

THE COURT: But, actually, and this is jumping around with you a bit --

MR. BOIES: Yeah, sure.

THE COURT: You know, the nature of the information, I understand what you're saying, could be objectionable to a particular class member in terms of the nature of the information. But if it is ultimately anonymized, then why

should they care?

MR. BOIES: Well, I think there are two reasons. First, they don't really claim it's anonymized. They say pseudonymized.

THE COURT: That was a new word to me, but, okay.

MR. BOIES: It's a new word to me, too, Your Honor.

I'm actually told they didn't invent it, that it existed before, but they've certainly adapted it to a new use.

And the reason they don't say anonymized and they say pseudo-anonymized is because this is tied to the device identifier, and the device identifier can be tied to a person. Even if the device identifier could not be tied to a person, that device identifier is still a very personal identification.

For most people today their smart phone that they carry around is the closest thing they have to their diary. It contains all of their private information. It is what they use to make purchases, to have their -- to have their personalized information tied to their personal device is itself I think something that people are -- would be concerned about.

But in addition to that, there's more, because they can and do sometimes link the personalized device identification to the name. So what they've done is they've taken this information, and it could be linked to the person. That itself is going to be concerning to people.

I mean, suppose that somebody puts a camera in a changing

room at a retail store, and they don't tell anybody so they don't know what's happening. They collect all this information. And suppose they blur the faces. Does anybody think that people wouldn't find that offensive, particularly if they say they're not doing it?

The thing that distinguishes their cases -- well, several things that distinguish their cases, but one of the things that distinguish their cases, is that here, Google told people they weren't going to do it. And they didn't just say we're not going to collect your personal information. What they say is, for example, in our Exhibit 36, in the summary judgment submissions, screen 1. "Activity Controls. Choose the activities and information you allow Google to save." It doesn't say choose the personal information. It says choose the information.

And they keep talking about Google account. There's no reference to Google account on this first screen.

There is a reference to Google account on the second screen, screen 2. But, again, no reference to personal information. It says in order to -- you've got to check a box in order to "include Chrome history and activity from sites, apps and devices that use Google services." They're talking about all the app activity. All of the app activity is saved, collected, and what they're telling people is that we're not going to do it if you check this box or unless you check this

box. If you've got this turned off, we're not going to collect the information.

And the reference to Google account here is just -- is choose which settings will save data in your Google account. Google account is not defined there. And if you go to the definition -- what they call the definition, it's not really a definition, it's just describing some of the stuff that's in the Google account.

And then if you go to screen 3, okay, it says: "Information about your browsing other activity on sites, apps, and devices that use Google services," and then it says: "To let Google save this information," this information about the app activity. "To let Google save this information, Web and App Activity must be on." It doesn't say anything about we're only going to save -- we're only going to not save personal information. It's talking about app activity. "To let Google save this information, Web and App Activity must be on."

Now, let me go to the next page which is a help page, WAA help page, screen 3. This is docket 315-17, at 2. It says at the beginning "Find and control your Web and App Activity." And it says "Web and App Activity saves your searches and activity from other Google services in your Google account." Nowhere does it say or suggest that they're going to save it anyplace else. The suggestion that, well, we said we are not going to save it in your Google account, but that doesn't mean

we're not going to save it someplace else.

This is a statement to people that the only place they're serving it is the Google account. So this idea that, well, we reserve the right, even though we didn't say it, we reserve the right implicitly that we could save this information, this app activity stuff someplace else unless it was personal data. There's no support for that in the actual documentation that's here.

And then it says -- it lists all the -- "When activity is on, you can include additional activity like," and it lists a whole bunch of stuff. And then it says "Information about your browsing and other activity on sites, apps and devices that use Google services to let Google save this information, Web and App Activity must be on."

That's what they're saying, and that's what they're saying in the specific stuff.

Now, in the -- they talk about their general privacy policy. That general privacy policy, when you print it out, goes on for 27 pages. Now, there's stuff in there that they can quote, but there's also stuff in there that they ignore. I mean, for example, and I've got an extra up here, and this is from pages 2 and 3 of Exhibit 8. Exhibit 8 is the entire policy. It begins by: "When you use our services, you're trusting us with your information. We understand this is a big responsibility and work hard to protect your information and

put you in control."

And then it goes on to say later on: "And across our services, you can adjust your privacy settings to control what we collect and how your information is used."

And then again it later on it goes on to say: "The information Google collects, and how that information is used, depends on how you use our services and how you manage your privacy controls."

There isn't anything here that says yes, but this only has to do with your personal information. Other stuff we always collect, and you can't do anything about it.

They could have very easily put in here: By the way, except for personal information, whether your web activity is on or off, we're going to collect all that information and log it in. They could have said that.

And interestingly, in their brief they quote -- they haven't got this quote about their ad personalization, and they point out that people can opt out of ad personalization. And then they say, and this is on page 13 of their opening brief, they quote something that's in their privacy provisions: Quote, even if you opt out of ad personalization, you may still see ads based on such factors as your general location derived from your IP address, your browser type, your terms of search.

They could have done that with app activity. They could have just as easily said even if you turn off WAA, we may still

collect the following information. They could easily have said that. They didn't say that. In fact, what they said is that for us to collect this information, to let Google save this information, Web and App Activity must be on.

Now, on the question of intent, you notice counsel didn't go through any documents, internal Google documents talking about intent. I want to go through some of those. Let me start at my number 12.

This is an internal Google email, 2019, December, from a Google executive. "Isn't WAA-off supposed to not log at all? At least that is what is implied from the WAA page." This isn't counsel's argument. This isn't counsel making it up. This is contemporaneous Google.

Let's go to the next page, November of 2019, a different Google software engineer and copying a whole lot of other people: "I think teams should not use user data at all if WAA is off. It's what I would think most users expect." This is not counsel trying to put a gloss on what they say. This is Google's internal statement.

Now, not only that, they did a study --

THE COURT: Let me first stop you on the two that you've mentioned.

MR. BOIES: Yeah. Yes.

THE COURT: What was the context in which these statements occur? Are there responses to the statement, and

who are these people in the hierarchy?

MR. BOIES: Sure. These are software engineers.

THE COURT: Okay.

MR. BOIES: And these are people who, in varying -- I'm going to go through a number of these people, but a number of these people are people who are related to the software engineering, they're related to trying to make the statements correct, and they're trying to figure out what they can use. These are people who see this information and they're questioning whether they can really use this information.

And Google says, well, these people didn't know what they were talking about; they were outliers. They can argue that to the jury. But certainly at the summary judgment stage, the fact that we have these internal documents, at a minimum, you know, creates a triable issue of fact. And there are a whole lot of them.

And if we go to the next page, there's Exhibit 3 in our summary judgment submission. This is a report. They did a study. They said: "In this study we want to get an understanding of users' mental model of the control hierarchy and see if users have a correct understanding of the relationship between the different controls on the page."

So they're doing internal research. This is in April of 2020.

And research question number 1. "WAA: What do users

expect turning WAA-off to mean?"

Answer, next page:

"All participants expected turning WAA toggle off to stop saving their activity."

Now, they're going to say, well, there weren't very many people in the survey. Google picked the number of people that were in the survey. This is what Google was internally relying on.

Now, after that, after that they decided to do a more detailed study, and this is Exhibit 41, and this is going to be research how they -- about how the design of a page impacted reading behavior. And they developed a hypothesis they were going to test. The hypothesis was based on the prior study, okay? The hypothesis -- and this is June of 2020. The hypothesis was: "Most respondents will believe that turning off WAA will result in no data being collected from their activity."

That's what they hypothesized their user -- that's what their intent was. That's what they internally believed.

Now, we never got the answer to this --

THE COURT: Well, now, stopping on that, it then goes on, there's a sentence that says "being collected from their activity and no personalization from Google products and services."

MR. BOIES: Both. Both.

THE COURT: Well, that's my question.

MR. BOIES: It's not --

THE COURT: You are distinguishing between the two.

MR. BOIES: Yes.

THE COURT: Okay.

MR. BOIES: As Google did.

And Your Honor makes a very good point. They didn't say most respondents believe there will be no personalization in Google products. They said: "Most respondents believe no data being collected from their activity, and no personalization." So they believed that neither of those things are happening. And, again, they've got some arguments on this, but those are for the jury.

Now, I want to go on next to page 33 in the evidence I want to go through.

This is another -- this is Mao Exhibit 2 in our summary judgment submission. This is another software engineer --

Oh, before I do that, though, before I do that, I just want to remind the court in our -- in our papers, Mao Exhibit 4, and I think 47, we have quotes from Google's CEO testifying at a House Judiciary Committee hearing in December 2018, and I think I've got -- yeah, yeah, here it is. Yeah, number 18. They put it up.

I'm not going to go all the way through it, but at the end it says: "We are pretty explicit about data which we collect

and we give protections for you to turn them on or off."

There's nothing here about saying we give you control of your personal information, but everything else we're going to take. That's not what they were saying.

But now let me go to page 33. This is another internal email, July 25, 2019. This is from another Google software engineer: "The WAA and other controls imply we don't log the data, but obviously we do."

He goes on to say: "I see how the wording here is very deceptive."

He goes on to say: "The user has a false sense of security that their data is not being stored at Google, when in fact it is."

That's not something counsel is making up. That's what Google is saying contemporaneously internally.

The same person: "We don't accurately describe what happens when WAA is turned off."

Again at Exhibit 2, same person: "We need to change the description."

If you go to chart 37, this is Mao Exhibit 59, at 46, a different Google employee: "WAA - completely broken, no way for the user to determine what this actually controls."

Mao Exhibit 64 on my chart 38, another Google employee, July 14, 2020: "To me, it feels like a fairly significant bug that a user can choose to turn off WAA but then we still

collect and use the data."

Now, throughout this there's no suggestion here, well, they're only talking about personalized data. There's no suggestion here that the data is just collected and then set it aside and never used in any way. This is what they're saying internally, Your Honor.

And, again, we can argue back and forth about the significance of some of these people, but at a summary judgment stage I respectfully suggest this has got to create at minimum a triable issue of fact, and I think in front of a jury they're going to have a hard time explaining some of these things.

THE COURT: Okay. Let's -- can you move for me to the harm issue?

MR. BOIES: Sure.

First, this here is -- there is a market for the plaintiffs' data, and that also distinguishes this case from the cases they're citing.

THE COURT: And elaborate for me "the market."

MR. BOIES: Sure.

THE COURT: You've done it in the papers, and I think I have a sense of where you're going with it. But humor me, give me sort of a summary of what this "the market" is here.

MR. BOIES: Sure. For example, Google itself -- and the Court in a similar case, *Brown against Google*, had the same issue and relied on the fact that Google had itself created, in

effect, a market.

And if you go to my chart, 42, which is an excerpt from the damages expert's report, and there was a survey that Google did and it paid users $3 a month to track their activity on their mobile phones and tablets. And the Court in *Brown* held, and we think pretty obvious, that when you're paying somebody for the data, you're putting a value on that. And this is data that with the WAA off, they took. It didn't belong to them. Belonged to the user. They took it. They told the user they weren't going to do it.

And the harm here is not just the harm of having your personal data taken. We think that's enough. And one of the things I think is significant is, and probably the farthest a court has gone that requires standing, is *TransUnion*. And in *TransUnion*, both the one thing that -- maybe it's not the only thing, but certainly one thing, and there weren't very many, that both the majority opinion and the dissent agreed on was that you could go after intrusion of exclusion and privacy. They said those were traditional kinds of harms that you could go after. So that if you had an intrusion, you didn't have to prove a monetary damage or something like that.

And as the court indicated earlier in prior opinions in the class certification motion to dismiss, one of the things we seek is nominal damages. And so nominal damages, when you have as many class members as we have, can be a very substantial

amount of money.

So there are all sorts of harms here that are cognizable.

And in addition to the price of a data, in effect, the value of the data that they improperly took, there's also a disgorgement and unjust enrichment. And you have a -- and the court will remember they had a *Daubert* challenge to that calculation, which the court rejected.

Now, they'll be able to argue that we're asking for too much. That's fair jury argument, and maybe the jury comes in somewhere in between. But in terms of allowing us to get to the jury, I mean, the court has already addressed the *Daubert* challenges, as to whether this is an appropriate thing to present, and it certainly is a quantification of the unjust enrichment that they have gotten.

So you've got your cause of action, you've got your liability, and you've got these means of measuring damages.

THE COURT: Well, to drill down a bit more on these different avenues that you've identified for me in terms of how we can -- how I can be comfortable to let the case go forward with this damage, these damages being requested. First you say there's a market for this, and that's reflected, as you've just pointed out to me, in Google's own payment to effectively get this material or a similar material. But that's -- isn't that a bit of a one-off?

I mean, if Google itself wants to run some analyses on its

operations, is that really -- you say they pay Google users $3 a month. Does that really establish a market, if you will, for -- that I could look to that says, well, okay, they've quantified the value of this information. They've done kind of a one-off study for their own internal operating. It's not like anybody in the outside world is -- outside of Google is paying this.

MR. BOIES: Well, actually, I think the evidence will be that other people like Neilsen and -- I mean, I think our expert goes through --

THE COURT: True. Okay. All right. Fair enough.

Then with respect to the emotional -- this is an issue that, as you know, we just wrestle with over and over again when we're talking about a class case. Can emotional distress be effectively a damage theory on a class-wide basis?

I understand emotional distress is available for invasion of privacy. No one can argue with you on that. And I know we're not talking about class certification at the moment. We've done that. But is it a viable -- if that were the only basis you could point to for a damage recovery, emotional distress, can that be done on a class basis?

MR. BOIES: Your Honor, I think if that was all we had, I don't think we could get more than nominal damages on a class-wide basis.

THE COURT: Okay.

MR. BOIES: I think in terms of quantification, I think the emotional distress, other than nominal damages, which I think we would be entitled to get, I don't think we could do that on a class-wide basis.

THE COURT: Okay. So you're using that as the predicate for the nominal damage recovery that you see?

MR. BOIES: I think that would be a predicate. That would be one predicate.

THE COURT: Okay. And then in addition to that there was a third avenue that you, I think, were identifying as a damage approach.

MR. BOIES: And that was on the harm to the devices.

THE COURT: All right. Harm to devices. And that's the battery degradation and the like, and I did have a case on that issue, yeah.

MR. BOIES: Right. And now, and don't put this one up. They want to -- this is quotes from something that they want to have sealed.

But if you turn to page 49 in what you have --

THE COURT: Okay.

MR. BOIES: -- at the top you have our expert, and that's not sealed. But at the bottom you have a quotation from Google's internal documents that --

THE COURT: Well, I'll just say I don't -- looking at this now just for guidance for the parties, I don't see any

basis to seal this, but that's a different question.

MR. BOIES: Yeah, I didn't see any basis either.

THE COURT: I know you're doing what you have to do, but, go ahead.

MR. BOIES: But, I mean, this demonstrates, we think, that Google recognizes that to the extent that it is doing -- collecting this data while WAA is off, that it has an effect.

Now, again, this is not something that we quantify. This is something that is a basis for nominal damages, basis for liability, but we can't quantify it on a class-wide basis.

You know, so we think there are those kind of -- we think there are those kind of harms.

And if I could maybe just spend a moment on the offensiveness --

THE COURT: Yes.

MR. BOIES: -- aspect of it.

THE COURT: I'll candidly tell you, I think that's -- that's a tough one for your side, because what I see is not obvious to me where one could couper up a highly offensive characterization.

MR. BOIES: Well, and I think that the offensiveness comes from a number of standpoints. I mean, first, I showed you the Schneier report where it goes -- has the kind of information that is being, you know, and I just -- think about it in any other context. If somebody was taking pictures of

you, you know, tracking you around physically for this kind of information, it would clearly be highly offensive. And the question is whether you can do -- and it's no less highly offensive because it's done electronically.

Now, the question is whether they have permission to do that, whether there's consent to do that. But if there's not consent, if there's not permission, this is clearly, I suggest, and certainly is a triable issue that this is highly offensive.

The second thing about it is that they ignored what they were being told internally by their own software engineers about what normal reactions were going to be, what normal expectations were going to be. And it's not just a handful of engineers. You'll see from this there are a lot of them. And in addition to that they did studies. These were not random emails. They did studies that came up with the same conclusions.

So you had not only the collection of stuff that they told people they weren't going to collect, but the character of what they were collecting was very personal. And they knew what they were doing, you know, at least there is a jury argument that they knew and were on notice to what they were doing.

They made very large profits from this. I think that goes into the offensiveness --

THE COURT: How --

MR. BOIES: -- calculation.

THE COURT: How do they really -- I understand you have your disgorgement theory. How do they make large profits from this. This being, I assume, the information you're saying that they are, in an anonymized way or otherwise, collecting. How does that then connect up to the large profits that they were making? I know you have expert information on this that theorizes it, but what --

MR. BOIES: Well, there's expert information, but also there's what we -- what we know that they do. I mean, for example, it's not just our experts. Their own -- their own documents, and to some extent their own interrogatory answers --

Let me see if I can -- I think I've got something in here that actually addresses, you know, that issue.

If I can go to page 21. This is from Google's responses to interrogatories in this case. This is Google's Fourth Supplemental Responses and Objections to Plaintiffs' Interrogatories, Set One, at 16.

> "Google uses user data collected via GA for Firebase across teams for product development, improvement, and diagnostics."

So it's not just putting it on the shelf. Google's response to Interrogatory 14, at the end it goes through all the logs. It says:

> "Google has provided exacting details of its main

logs associated with the transmission of app-interaction/measurement data to Google via Google Analytics for Firebase when a user has turned WAA off."

So we're talking about when they've turned WAA off. It then says:

"Google states, however, that it is not practical or relevant to account for every single potential data source (including logs) that may contain such data because there are various downstream users of the pseudonymous data."

Okay. Various downstream uses, so many that they can't even count them. They can't even tell us in an interrogatory.

The Hochman report, our expert report, at paragraph 273 is the one I've got here, where it says:

"Google's collection of WAA/sWAA-off data also enables Google to serve targeted advertisements."

We took a deposition of a former Google software engineer, Blake Lemoine, and he testified about how they used WAA-off data for their AI.

The Hochman report, paragraphs 102 and 305, also have additional detail.

But interrogatory number 15, if I can go to my chart 28, we said interrogatory 15:

"Please describe how Google currently uses and previously during the class period has used WAA-off data."

So -- and you'll see the response is here, and they say at

the end, and I've highlighted it on the screen, but they say at the end that the use "includes pseudonymous conversion tracking and ad targeting for anonymized ad profiles." So they're using it for ad targeting.

Now, they then gave a supplemental response to number 15, which is at docket 364-22, at 9 to 10, in which they gave additional examples of how they use this -- they use this information.

THE COURT: But then the -- is the premise that because they used the information, somehow then all the profits they make are ascribable to this?

MR. BOIES: No. No.

THE COURT: Okay. Well, and that's where your experts do their calculation.

MR. BOIES: Exactly. No, no, we're not claiming all their profit. I mean, the $644 million, I think that may be a daily profit for them. I don't know how much they make, but they make so many hundreds of billions of dollars that --

THE COURT: So you're not asking for all of it.

MR. BOIES: We're not even asking for 10 percent of their profits.

THE COURT: Okay.

MR. BOIES: But what you can see is that there is enormous value, you know, in what is done. There are a lot of different uses.

They can argue to the jury, well, this wasn't all that valuable. Yes, we collected it, but we could have done it some other way, and the plaintiffs are asking for too much money. Those are all jury arguments. Those aren't -- and to the extent perhaps maybe a *Daubert* argument, but it's not a summary judgment argument. These are all pieces of evidence from which we can properly argue to the jury that they have taken something for which there was a market, for which there was great value to Google and value to the user as well.

THE COURT: Okay. Can I now turn to Mr. Santacana to respond?

And I referred to you as Mr. Salcedo. I apologize to Mr. Santacana.

MS. SANTACANA: Thank you, Your Honor.

I'd like to start where Mr. Boies ended on harm.

Your Honor, the data that we're talking about here, and there hasn't been a serious disagreement about this, is not a diary. It isn't a videotape of somebody even with their face blurred. The data here is a list of receipts that Google never uses but for the purpose of keeping records. That's the data we're talking about.

And when --

THE COURT: Does keeping records potentially have some value? Because you're then sharing this recordkeeping to assist, as I understand it, advertisers in what they're doing,

or at least to --

MS. SANTACANA: Yeah, report --

THE COURT: It can be described as, hey, you're doing a good job --

MS. SANTACANA: Right.

THE COURT: -- look at this.

MS. SANTACANA: Exactly.

THE COURT: It's to boost them up a bit.

MS. SANTACANA: Report the effectiveness of the campaign.

THE COURT: There you go.

MS. SANTACANA: Yeah. Absolutely.

THE COURT: Okay. So you sort of say, well, that's, you know, no big deal. It's kind of just recordkeeping. But to share it with them sort of implies to me that you think there's some value to it.

MS. SANTACANA: Your Honor, I mean, I think you're using some value to it, I guess, in the colloquial sense.

THE COURT: True.

MS. SANTACANA: The question on this motion is not whether there's value to Google, but whether there's harm to the class that is provable on a class-wide basis.

THE COURT: Well, although we would get to the value issues when we're trying to quantify the harm.

MS. SANTACANA: If there is any harm to begin with,

sure. But I'm saying there's no harm to begin with, right? The activity of keeping an anonymized receipt that an ad was served is not harmful to anyone. And if it were, there would be evidence of it that someone other than these plaintiffs' counsel cared about it.

Not even their clients cared about it when they testified. What their clients cared about was personalized advertising. That's what they testified about: I don't want you to know everything I'm doing, and send me better ads when I turn WAA off. One of them said I do want you to do that, but not when I turn WAA off, and then the rest said I never want you to do that.

We're not doing that. We said we wouldn't. We're not doing that.

When we're talking about a market for data, I'm aware of four -- sort of four leading cases on the question of whether you can get past, on the tort claim and on the CDAFA claim, the filter of Rule 12 or Rule 56 with a market for data. Two of them are yours, *Katz-Lacabe* and *Williams versus Facebook*, one of them is Judge Chhabria's in *McClung versus AddShopper*, I think it's called, and then the *Hazel* case by Judge Breyer. They all come out the same way. The only case that comes out the other way is *Brown*.

And in *Brown*, which is the one plaintiffs hammer on, they are the plaintiffs' counsel in that case, what Judge Gonzalez

Rogers was evaluating was an allegation that browsing histories were being collected and incognito mode. This case is not about browsing histories. The allegation in *Brown* is that they were then being used to target advertising. This case is not about browsing histories being used to target advertising.

It is undisputed -- their own expert says we don't personalize advertising with sWAA-off data. In the second paragraph of their class certification motion they actually accuse us of being deceptive by not personalizing advertising with WAA-off data. They say because if we did, then it would tip off the plaintiffs that we are using it for something, that we have saved it, but now, at summary judgment, they're telling you that we are, with no evidentiary basis.

So on the market for data, what they've done is convert what is really another disgorgement theory into a theory of actual damage. And the way it goes is, well, Google is paying or Neilsen is paying or somebody is paying people for their browsing histories. Again, this case is not about browsing histories. We're not using browsing histories for anything that are sWAA-off.

But in any case, they can sign up right now for Google Screenwise program and they can get their $3 per month right now. The value of their data has not diminished one iota. Google has not stood in their way of selling their data. And since Google isn't using browsing histories, like the ones that

are collected in the Screenwise program for any purpose, such as to profit, Google is not also causing any harm to them by getting away with stealing something that they could have paid for.

So it is a complete misnomer to point to that program and say --

THE COURT: Well, I'm having trouble with your argument to the extent you're saying, well, they haven't been harmed because they can go out and get the $3 a month today. But that's not really the question, is it? It's the $3 a month is being pointed to by the plaintiffs to me to show that there's some value to this. The harm could -- maybe they don't want to sell it, but the $3 a month is just -- is putting some value parameter to show that it's not worthless --

MS. SANTACANA: Yes.

THE COURT: -- information. But is it enough to say, well, they're not harmed, because if they really want the money they can go out and get it. That's really kind of beside the point.

MS. SANTACANA: No, it's not. And this point puts the lie to their damages model, because what they're saying is if it has value in the abstract, then I must have been harmed.

But the claims require harm. They're not -- the claim says actual damage or loss. Okay. What was the damage? What was the loss? Did they lose --

THE COURT: Let's posit a person who says: I absolutely don't want my information to be shared with anybody. And then the question is -- and a lawsuit is brought, and you say, well, no harm, no foul, this is valueless information. And so then they come back and say, no, look, there is a value to this, but the individual that we represent, it doesn't -- there's harm to them because information that is of value is being used and they don't want it to be used.

MS. SANTACANA: Yes. Control over their private information.

THE COURT: So, and you're saying, well, but they can't be harmed because they can sell the information. They haven't, you know, their information is just as valuable today as it was when we did what we were alleged to have done. But that's ships that are passing in the night. That's not going to the question of, you know, is there a value in this, whatever the person wants to do with the information.

MS. SANTACANA: So the -- I don't think it's ships passing in the night. I think the issue -- this is exactly my point, is that what you just articulated is a desire to control private information, which is the traditionally, you know, the restatement talks about this. This is what invasion of privacy torts are all about. And the harm is the emotional distress that is caused by preventing me from being able to control it. And then you say how do I measure that harm? And it would be

unusual to say, well, if you had sold it, it would have been worth X, Y and Z.

Now, you might say I want disgorgement as a form of relief or you might --

THE COURT: Or one could also interpret that as being an answer to your claim that no harm, no foul because this is worthless. And they're saying it's not worthless, in fact, there's a market out there.

So, and that's answering that question. It's not going to the issue of -- unless they want to sell it they can't be harmed.

MS. SANTACANA: Yeah, and I think maybe I'm not --

THE COURT: I understand. I think I know what you're trying to tell me, so we can move on to the next point.

So go ahead.

MS. SANTACANA: Okay. Well, to jump off of that point, I heard nominal damages come up I think four times when counsel was speaking. That's four more times than it came up in the briefing, so this is a little bit fly-by-the-seat-of-the-pants.

But here's the problem with the reference to nominal damages. The Supreme Court for the longest time, going back to *Amchem versus Windsor*, Justice Ginsburg's opinion, says, effectively, personal injury is a pretty dangerous place for class actions, for a lot of reasons.

What you just heard counsel say is even if you don't believe me on the market for data, even if you don't believe me on the battery depletion, even if you don't believe me on disgorgement, I should still be able to go to trial and collect, presumably, they will say, a penny for each class member, or some amount of nominal damage, which I don't think is the law anyway. It could be just one dollar for the entire class.

But in *Amchem*, what the Court says is, well, hold on a second. If your claim is that some people in this class suffered emotional distress, now you aren't representing them adequately, because that means that you are asking only for nominal damages for someone who suffered actual harm. This is why we don't do this in class actions unless in the most clearest of cases.

So the nominal damages piece is not a loophole to get around what is clear case law from the Supreme Court, *Comcast versus Behrend*, *Amchem versus Windsor*, *Fibreboard versus Ortiz* that says when you're doing damages in a class you have to be careful, the model has to match the liability theory. And if you're dealing with personal injury, then you have to be careful about individualized issues.

That is why, Your Honor, at the class cert. stage in their brief they disclaimed any reliance on this. Mr. Boies was talking about emotional distress and saying he can collect

nominal damages, but in their brief they disclaim this. And I can give you the page cite if you'd like it, but I'm sure you remember the hearing. They said: I don't have to do that type of damage. What I want is disgorgement. Well, then *TransUnion* is decided and *McClung* is decided and now disgorgement doesn't look so good, so now they're talking about nominal damages again.

THE COURT: You want to address for me the anecdotal, in the sense --

MS. SANTACANA: Yes, I do.

THE COURT: -- information from some of your people --

MS. SANTACANA: Yes, I do want to address it.

THE COURT: -- that Mr. Boies drew my attention to.

MS. SANTACANA: Yeah. Your Honor, these emails are trotted out in every one of these cases. This is a 150,000-person company. I think, as you pointed out, context is probably the best way to weed out ones that matter from ones that don't, ones that are relevant from ones that don't. Half of the ones he showed you he also showed Judge Gonzalez Rogers in *Brown*, which has nothing to do with this case.

So the other half are seriously flawed, and I am happy to go -- I could go through each one right now if that's what you want.

THE COURT: Well --

MS. SANTACANA: But at a more general level --

THE COURT: Yeah.

MS. SANTACANA: -- to be hopefully more helpful to Your Honor, the problem with that evidence is that not one of them addresses the specific conduct that is being sued upon here. And by their logic, they could sue Google over and over again as to WAA in each one of every aspect they can come up with if anybody ever found WAA confusing as to some other aspect.

So I find that's one problem with it, because WAA is actually a very capacious button. You've seen the description: Chrome history is in there, sites are in there, app data is in there - there's all kinds of stuff in there. So, you know, that could become a cottage industry in and of itself if these 12 emails are sufficient to get past summary judgment.

THE COURT: Well, you know, it really, to some extent, goes back to my initial question to you, which is from a very, very simplistic level, what I understand the plaintiffs to be saying is certain of their class members are operating on the understanding that even -- and this puts aside your issues with respect to the language of the privacy policies and the like, but that they think they have exited any use of anything anonymized or otherwise about them. And some of those emails, whether or not they, you know, are applicable in all sorts of other cases, they go to that question.

MS. SANTACANA: Yeah.

THE COURT: They go to the issue of saying the consumer out there thinks they've checked out, and they haven't. Pretty simplistic thing. But just because those emails may have applicability in other lawsuits doesn't mean they get disregarded in this one.

MS. SANTACANA: The point is well taken, and I think the best way to address that is to address an example.

So four of the examples you were shown or four of the slides you were shown were all authored by an employee named Chris Rumler, who comes up in every one of these cases. The plaintiffs all over the country love Chris Rumler and his colorful emails.

And what Chris Rumler was talking about in these emails, he was really upset about it over the course of months, he wrote email after email after email, and this is what he testifies to. It's in the record, we put in it there. He works on Gmail. There's only one kind of data in Gmail - data tied to your identity. That's how Gmail works. This is like a foreign concept to him, that there's such a thing as anonymized data, because it doesn't -- it didn't enter his mind. And so he's asked about it by these lawyers, and he explains that: I read a technical proposal from a different product team I know nothing about. I misunderstood it to mean that Google was going to identify data in a log with the person's GAIA ID, which is basically their email address, their Gmail address,

even when WAA was off, and I was really upset about that. Which is exactly what Google wants its employees to do, is be on the lookout for this sort of thing. And once it was explained to him, and once he understood the proposal, he changed his mind. He has disavowed the plaintiffs' view.

THE COURT: Now I'll ask you the question you know is coming on summary judgment --

MS. SANTACANA: Sure.

THE COURT: -- which is that's all well and good, but why should that be the only interpretation that is adopted such that --

MS. SANTACANA: Right.

THE COURT: -- the obvious alternative interpretation of those, some of those statements is disregarded? I mean, isn't that something for the jury to hear what you just said about explaining the Rumler comments. And you'd be perfectly free to have this individual on the stand and to explain it exactly as you just have explained it. But on summary judgment isn't it a tall order to say that I have to adopt that interpretation? Because the counter --

MS. SANTACANA: I don't think you do.

THE COURT: -- the alternative interpretation is what I said before, that it is indicative of or supportive of the argument, from a macro level, that the plaintiffs are making that their class members think they're out from under, and even

within Google there are people who are saying that's what they think, and that's not what's happening.

MS. SANTACANA: Right.

THE COURT: I mean, it's pretty simplistic, I understand, and you have all sorts of reasons why context matters, and it's not what you think it is, and all that, and I'm not surprised. But, you know, I am at summary judgment so...

MS. SANTACANA: I understand, and credibility is generally a trial issue, and I'm not asking Your Honor to adopt a particular interpretation of the statements. I'm just putting them in context of the record evidence. That's all I'm doing, because you requested it.

But on the legal question of consent, which I think is what we're talking about right now, I do not think that Chris Rumler's statements undermine the plain language of the disclosure and the privacy policy, and I -- because they can be read consistent with what we're saying it means. And what they're saying it means cannot be reconciled with the plain language.

Again, it doesn't say you are out from under, nothing -- this android device will just shut down and not send anything to Google ever about anything. We won't save anything.

I'll just give you a ridiculous example, right. If a user turns WAA off on their android device and then downloads an app

in the Google Play Store, under plaintiffs' theory of what is a reasonable reading of WAA, Google would not be permitted to keep a log that that device downloaded that app.

If that same device then pays for something using Google Wallet on a web site, according to them Google would be disabled from keeping a record that this user used Google Wallet to pay for this item on the Internet.

If that same user then logged into Google and sent an email through Gmail, under their theory we would then have to delete that.

THE COURT: Of course under all of those examples Google is retaining the information, not sharing it with anybody else.

MS. SANTACANA: Nor is -- well, it's not sharing -- I guess I don't understand your question.

THE COURT: Well, in this particular scenario the, as I understand it, the anonymized data is ultimately going to advertisers in the form of saying, look, your ads are working. This is good -- the information is being utilized by Google outside of Google.

MS. SANTACANA: There's no evidence that Google is sharing individual level --

THE COURT: Oh, I understand that. I understand that it's, if you will, being packaged, but the information is being -- is being characterized by Google to third parties in

the form of saying, look, your ads are working.

MS. SANTACANA: Sure.

THE COURT: And some of the information that goes into that communication is this anonymized data.

MS. SANTACANA: Well, I guess I'm not sure what connection that has to the description of WAA, which is not -- is not talking about whether we will or won't share aggregated information with advertisers -- that's sort of orthogonal, I think, to the --

THE COURT: So you're saying that under their reading there's a violation -- you would be violating the policy even if there is operational information that's -- that at a certain period of time is within Google. I understand what you're saying, right.

MS. SANTACANA: Yeah, I mean, the guy who sold the sneakers to the user --

THE COURT: Got you. Yeah, I understand.

MS. SANTACANA: So just a couple more points on this, Your Honor.

First, I just want to be clear, Google doesn't share the device identifiers with advertisers. So whether it's a consent question or a --

THE COURT: You get into the *could* issue, which we've already hashed out.

MS. SANTACANA: Okay. Well, if you feel like we've

hashed it out -- I felt like I heard something relatively new, in that, the argument you asked counsel if it could be but it never is and it never has been, is that still actionable?

THE COURT: Mm-hmm.

MS. SANTACANA: On that, just on that question I think there's significant case law that says no, it's not actionable.

And whether you want to analyze that under harm or expectation of privacy or even just under the consent rubric, depending on the case it comes out in different places, but the *Hammerling* case, which is affirmed by the Ninth Circuit, is one of them that analyzes it on consent.

And there's a couple of others in our papers.

THE COURT: Mm-hmm.

MS. SANTACANA: So I just think that would be stretching the law to a place it hasn't gone to before, and there isn't a case that's been cited on that basis.

The *Brown* case doesn't go that far either. The *Brown* case says this is a browsing history that's -- that is identifiable because it's an entire browsing history. Where, as here, what we're talking about is the record of ad service.

THE COURT: *Hammerling* was a non-published --

MS. SANTACANA: The panel decision is unpublished, yes. And the lower court decision makes the same ruling. That's why I say it was affirmed, but --

THE COURT: I understand.

MS. SANTACANA: -- not published.

Okay. So the last point I wanted to make, Your Honor, is about the privacy policy.

The plaintiffs rely on the privacy policy to make their claims, while at the same time arguing that we shouldn't assume users read it. But the plaintiffs who testified each testified and submitted declarations, which we have in our papers, that say "I read and relied on the privacy policy."

So I understand it's a legal fiction that, you know, people read all the terms of use and all these things. But in this case the testimony from the plaintiffs is: I read it and relied on it, that's why I'm here.

So yes, I could pick out phrases that are ambiguous if read in isolation, but I think at a minimum the court should analyze the WAA disclosures and the privacy policy together holistically. And when done that way, one thing is very clear. Mr. Boies said Google could easily say there's such a thing as not your personal information. We say that. We say it in the privacy policy over and over and over again and provide a definition that distinguishes personal information which is associated with a Google account from non-personal information which we say cannot reasonably be linked to your identity.

So we do say that in the privacy policy, and I do think that has to be -- and it may be 27 pages long -- we say it at least every couple pages, and that has to be part of the

analysis.

And if, if this motion comes down to, well, there's a fact question about whether it can reason -- it could reasonably be linked to your identity by somebody somehow someday, as I said, I don't think the law supports that on the consent side. It definitely doesn't support it on the harm side, Your Honor. Because even if it could reasonably be linked, a browsing history that falls in the woods can't hurt anybody.

And it may be that one day somebody can point to actual harm, but as of today, looking back, class wide, Google kept its word.

Thank you, Your Honor.

THE COURT: Thank you.

MS. SANTACANA: Yeah. Actually, I'm sorry, can I address one more thing?

THE COURT: Yeah, go ahead.

MS. SANTACANA: So Mr. Boies showed you an interrogatory response. I don't know how much weight Your Honor would put on that, but I want to make sure it's clear to Your Honor that that interrogatory response that he showed you, which says that there's such a thing as anonymized ad profiles, it is explained in the supplemental response and also in deposition testimony that that was an edge case where somebody is sharing their device in a signed-out state, and the owner of the device has WAA off, but the device doesn't know that when

they're sharing it with somebody else.

So it's really not a class-wide issue. They're edge cases where if somebody -- if people are sharing tablets, it's unclear which account is going to control the way the data is treated, and that's all that was meant by that.

So I'm not sure the court should put any weight on that.

THE COURT: Okay. Thank you very much. Very helpful argument.

I'll take the matter under submission and get you an order.

MS. SANTACANA: Two housekeeping things, Your Honor.

THE COURT: Yes.

MS. SANTACANA: So first, because of the class notice schedule, we wanted to make sure Your Honor is aware that a summary judgment order probably should not issue, I think best practice is not to issue before the opt-out period closes. The parties are agreed on that.

By our calculations we're looking at sometime in January, maybe late December, if we're lucky, is when the opt-out period will close, and right now trial is scheduled for early February.

So we've lightly talked about what we should do but wanted to sort of put it on your radar that we may need to move the trial a little bit, and we're not sure what your schedule looks like.

THE COURT: Right. Well, I've got a criminal trial in February, so you'll be moving, if February was the real date, in any event.

But does it matter whether or not I'm granting or denying? I mean, if I'm denying summary judgment, the timing is --

MS. SANTACANA: Would matter less? But I don't think Your Honor should indicate his intentions before the opt-out period closes.

THE COURT: Which is January?

MS. SANTACANA: It creates incentives around whether to opt out.

THE COURT: All right. And that's January, when is it?

MS. SANTACANA: Most likely January 6th, you know, maybe a week sooner or something.

MR. BOIES: I think he's right. If it should be December or -- we have some issues that we'll continue talking about.

The data they've given us is not really very useful in terms of making the -- getting the stuff out, so it's taking longer than it should have.

THE COURT: Okay. Well, you know, when counsel asks me please don't rule for a while, I don't mind that. That's fine.

(Laughter)

THE COURT: But it does -- you know, this issue does not -- it's a bit academic, because I, frankly, wasn't even focused on the February trial date in this case. But that's not -- that's not a realistic date for my schedule, so we're going to have to reassess that in any event.

But I'm happy to -- I'm happy to hold off a pending -- the parties will -- can the parties agree that they can give me the trigger of, okay, you know, we've passed the date -- and I understand the reason why, because, you know, binding class members and the like. But I'll leave it to you to tell me so it doesn't just fall through the cracks and I'm doing other things.

MR. BOIES: We can do that.

MS. SANTACANA: Sure. Absolutely, Your Honor.

THE COURT: Okay. Very good. Thank you.

ALL COUNSEL: Thank you, Your Honor.

(Proceedings adjourned at 3:17 p.m.)

CERTIFICATE OF REPORTER

I certify that the foregoing is a correct transcript from the record of proceedings in the above-entitled matter.

Dated: July 26, 2024

Rhonda L. Aquilina, CSR #9956, RMR, CRR, CRC
U.S. Court Reporter